AMENDMENTS TO THE CLAIMS

Please amend the claims as follows:

1. (Currently Amended) A method for conveying a security context, comprising:

obtaining a virtual address associated with a process executing on a recipient computer system;

issuing a first Internet Protocol version compliant packet, wherein the first Internet Protocol version compliant packet comprises a first Internet Protocol version compliant header, wherein the first Internet Protocol version compliant header comprises a security context, wherein the security context comprises a Supernet identifier, a Channel identifier, and the virtual address, and wherein data in [[the]] a payload of the first Internet Protocol version compliant packet is encrypted using the Supernet identifier and the Channel identifier to obtain an encrypted payload;

issuing a second Internet Protocol version compliant packet, wherein the second Internet Protocol version compliant packet comprises a second Internet Protocol version compliant header, wherein the second Internet Protocol version compliant header comprises a second Internet Protocol version compliant address of the recipient computer system, wherein a payload of the second Internet Protocol version compliant packet comprises the first Internet Protocol version compliant packet, and ~~prepending an issued packet with a second Internet Protocol version header producing a second Internet Protocol version compliant packet,~~ wherein the first Internet Protocol version is different from the second Internet Protocol version; and

forwarding the second Internet Protocol version compliant packet to the recipient computer system,

wherein the security context is used by the recipient computer to decrypt the encrypted payload.

2. (Original) The method of claim 1, wherein the first Internet Protocol version compliant packet is Internet Protocol version 6 compliant packet.

3. (Original) The method of claim 1, wherein the second Internet Protocol version compliant packet is Internet Protocol version 4 compliant packet.

4. (Previously Presented) The method of claim 1, wherein issuing the first Internet Protocol version compliant packet further comprises:

invoking a Supernet Attach Command on an authentication server daemon;

receiving, in response to the Supernet Attach Command, Supernet configuration information comprising the security context; and

registering a mapping of the Supernet configuration information with a virtual address daemon.

5. (Cancelled)

6. (Previously Presented) The method of claim 1, wherein the security context comprises a 128 bit unique value.

7. (Previously Presented) The method of claim 6, wherein the 128 bit unique value comprises a 16 bit set and a 112 bit set.

8. (Original) The method of claim 7, wherein the 16 bit set denotes a site local Internet protocol address comprising 12 bits for an address prefix followed by 4 bits for a zero value.

9. (Original) The method of claim 7, wherein the 112 bit set comprises contiguous bits for the Supernet identifier, the Channel identifier, and the virtual address.

10. (Original) The method of claim 7, wherein the 112 bit set comprises a 64 bit Supernet identifier, a 24 bit Channel identifier, and a 24 bit virtual address.

11. (Original) The method of claim 4, wherein the virtual address daemon maps the virtual address of the recipient process within the Supernet to an actual Internet protocol address.

12. (Cancelled) – 29. (Cancelled)

30. (Currently Amended) A method for processing a security context, comprising:

receiving a first Internet Protocol version compliant packet comprising a first Internet Protocol version compliant header and a first Internet Protocol version compliant payload, wherein the first Internet Protocol version compliant payload comprises ~~encapsulated by~~ a second Internet Protocol version compliant packet, wherein the ~~first~~ second Internet Protocol version compliant packet comprises encrypted data and a second Internet Protocol version compliant header comprising a security context, wherein the security context comprises a virtual address, a Supernet identifier, and a Channel identifier;

extracting the encrypted data and the security context from the ~~first~~ second Internet Protocol version compliant packet ~~encapsulated by the second Internet Protocol version compliant packet~~;

decrypting the encrypted data, by a recipient computer system, ~~in the first Internet Protocol version compliant packet~~ using the Supernet identifier and Channel identifier to obtain decrypted data; and

routing the decrypted data to a process in the recipient computer system using the virtual address,

wherein the first Internet Protocol version compliant header comprises a first Internet Protocol version compliant address used to route the first Internet Protocol version compliant packet to the recipient computer system.

31. (Previously Presented) The method of claim 30, wherein the security context comprises a 128 bit unique value.

32. (Previously Presented) The method of claim 31, wherein the 128 bit unique value comprises a 16 bit set and a 112 bit set.

33. (Previously Presented) The method of claim 32, wherein the 16 bit set denotes a site local Internet protocol address comprising 12 bits for an address prefix followed by 4 bits for a zero value.

34. (Previously Presented) The method of claim 32, wherein the 112 bit set comprises contiguous bits for the Supernet identifier, the Channel identifier, and the virtual address.

35. (Previously Presented) The method of claim 32, wherein the 112 bit set comprises a 64 bit Supernet identifier, a 24 bit Channel identifier, and a 24 bit virtual address.

36. (Currently Amended) The method of claim 30, wherein the security context is obtained from ~~first~~ the second Internet Protocol version compliant packet using a handler mechanism.

37. (Previously Presented) The method of claim 34, wherein the handler mechanism is a Netfilter.